

AMENDMENTS TO THE CLAIMS

1. (Cancelled)

2. (Currently amended) A method according to Claim + 16 wherein the ~~document~~ test certificate producer includes a bar code in the ~~document~~ printed test certificate, said bar code containing the authentication code, and wherein the ~~document~~ certificate checker is provided with means for reading the bar code to obtain the authentication code.

3. (Currently amended) A method according to Claim + 16 wherein the ~~document~~ printed test certificate includes a pre-printed serial number, which is sent to said authentication authority, and wherein said authentication authority uses said pre-printed serial number in generating said authentication code.

4. (Currently amended) A method according to Claim 3 wherein said pre-printed serial number is included in said ~~document~~ printed test certificate as a pre-printed bar code.

5. (Currently amended) A method according to Claim 4 wherein the ~~document~~ test certificate producer uses a combined printer and bar-code scanner to read said pre-printed bar code and then to print said ~~document~~ printed test certificate.

6. (Currently amended) A method according to Claim + 16 wherein said ~~document~~ certificate checker performs the following steps:

- a) entering said authentication code into a computer;
 - b) entering information in the ~~document~~ printed certificate into the computer;
 - c) causing the computer to cryptographically generate a check code from said information;
- and

d) causing the computer to compare said check code with said authentication code and to generate a warning indication if said check code does not correspond with said authentication code.

7. (Currently amended) A method according to Claim 4 16 wherein said authentication authority cryptographically generates said authentication code using a cryptographic key associated with said authentication authority.

C1
am4
8. (Currently amended) A method according to Claim 7 wherein said cryptographic key is a secret key known to both the authentication authority and said ~~document~~ certificate checker, but not known to said ~~document~~ test certificate producer.

9. (Original) A method according to Claim 8 wherein said authentication code is generated by performing a key-dependent one-way hash of said information, using said secret key.

10. (Currently amended) A method according to Claim 7 wherein said authentication authority generates said authentication code using the private key of a public/private key pair, and wherein the ~~document~~ certificate checker checks the authentication code using the public key of said public/private key pair.

11. (Currently amended) A method according to Claim 4 16 wherein communication between said ~~document~~ test certificate producer and said authentication authority is protected by encryption.

12 -15. (Cancelled)

16. (Previously presented) A method for authenticating a printed test certificate comprising the following steps:

- a) a test certificate producer performs a test and sends information to be included in a test certificate to an authentication authority;
 - b) the authentication authority checks whether the test certificate producer is authorized to perform the test and, if so, cryptographically generates an authentication code from said information, and sends the authentication code back to the test certificate producer;
 - c) upon receipt of the authentication code from the authentication authority, the test certificate producer prints the test certificate, including both said information and said authentication code; and
 - d) upon presentation of the printed test certificate for authentication, a certificate checker cryptographically checks the authentication code against said information in the printed test certificate to determine whether the printed test certificate is authentic.
-